UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

* *

UNITED STATES OF AMERICA, Ex Rel.
PATRICIA B. McINNIS and
TIFFANY D. ATKINS,

Plaintiffs,

vs.

NORTHROP GRUMMAN SYSTEMS
CORPORATION,

Defendant.

2:14-cv-1240
Judge Watson
Mag. Judge Abel

FILED IN CAMERA
AND UNDER SEAL
PURSUANT TO 31 U.S.C. §3730 (a)(2)
THE FALSE CLAIMS ACT

* *

COMPLAINT

TABLE OF CONTENTS

I.
INTRODUCTION

1. This case is brought by *qui tam* Relators Patricia B. McInnis and Tiffany D. Atkins (Relators), through their undersigned attorneys, on behalf of the United States of America. It is brought under the Federal False Claims Act (FCA), 31 U.S.C. §3729, et seq., to recover on behalf of the United States for false and fraudulent claims for millions of dollars by Defendant in connection with its contract with the United States for the Integrated Air and Missile Defense (IAMD) Battle Command System (IBCS).

2. The case arises from Defendant's continual billing and receipt for millions of dollars under the contract when it was failing to build in and produce required:

- Anti-Tampering Protections;
- Information Assurance (electronic security for preservation and security against intrusion, especially foreign intrusion); and
- Configuration Management (ensures changes occur only after thorough assessments of performance, cost, schedule impacts, and associated risks).

These protections are designed to prevent unauthorized transfers of military information and technology. Anti-Tamper is especially important to prevent reverse engineering of our military weapons and systems. The claims for payment under the contract were also false and fraudulent because Defendant engaged in a cover up of their failures to produce these necessary components, and wrongfully attempted to evade those necessary requirements mandated by the contract and federal laws in Department of Defense regulations, rules and clear instructions. These failures and cover up efforts, with the concomitant wrongful billings of the government, began at least by 2010 and are currently continuing in 2014.

3. Relators, who are very experienced in weapon system program development, firmly believe that if the flawed IBCS is deployed, it could result in the compromise of numerous missile defense systems, including the PATRIOT, Sentinel, Joint Land Attack Cruise Missile Defense Elevated Netted Sensor System (JLENS), Joint Tactical Ground Stations (JTAGS) and Terminal High Altitude Area Defense (THAAD). The missions of these systems are to engage incoming cruise missiles, Unmanned Aerial Vehicles (UAVs), and Tactical Ballistic Missiles (TBMs). These critical weapon systems of the U.S.A. could not only have their sensors disabled by an enemy, but could allow the enemy to turn the weapons upon U.S. or allied forces.

II.
PARTIES

4. Defendant Northrop Grumman Systems Corporation (hereinafter Northrop Grumman, Northrop or NG) is incorporated and maintains its headquarters in West Falls Church, Virginia. It produces a wide range of products and services in the aerospace, electronics and ship building fields, in the military air, land, sea and space systems. It is a global aerospace and military technology company, and in the top five largest military contractors in the world. Its reported revenues in 2012 were over $25 billion. The contract for the IAMD-IBCS at issue here is administered by Northrop's Information Systems Sector, which has annual revenues of approximately $7 billion.

5. Relator Patricia B. McInnis has over 35 years of experience in various systems engineering, industrial engineering and operations areas, including system security engineering, project management, risk management, education and training, test and evaluation, cost analysis, software engineering and design of experiments. The primary use

of her knowledge and skills has been in support of Department of Defense research, development and acquisition programs. Her background includes:

- Auburn University degrees in mathematics in 1970, Master of Education in mathematics/secondary education in 1974, and Master's Degree in industrial engineering in 1981;
- From 1981 to 1991 she was the proprietor of Psi Star Computing in Phenix City, AL, which provided data processing training and program development for clients;
- From 1978 to 1982, she was a college instructor in mathematics and computer science for the Alabama Junior College Systems;
- From March 1982 to October 1984, she was an industrial engineer for the U.S. Army at Fort Benning, GA;
- From 1986 to 1991, Ms. McInnis was a senior operations research and systems analyst for a major U.S. Army operational testing agency for a number of top priority operational testing activities for development of infantry weapons systems and equipment, at Fort Benning, GA;
- From 1991 to 1994, she was a senior cost analyst for the Multiple Launch Rocket System and Close Range UAV for the U.S. Army at Redstone Arsenal, AL;
- From 1994 to 2004, she was a systems engineer with the U.S. Army for the Tactical Unmanned Aerial Vehicle (TUAV) outrider project office in Huntsville, AL;
- From 2000 to 2004 she was a general engineer with the U.S. Army AMRDEC at Redstone Arsenal, AL on a variety of projects;

- From 2004 to 2008, she was a certified Technology Protection Engineer (TPE) in Huntsville, AL for the Army Research and Technical Protection Center DA G2;
- From February 2008 to January 2009 Ms. McInnis was a Systems Integration Engineer supporting NASA's Technology Protection Program with Concurrent Technology Corporation in Huntsville, AL;
- From June 2009 to March 2010 she was a Systems Engineer for AEgis Technologies Group in Huntsville, AL, in all aspects of program and technology protection planning, as the subject matter expert for the Integrated Air & Missile Defense Program Office (IAMD), where her duties included program protection integration into systems engineering management, test and evaluation, and program management, and she was a part of the Program Protection Working Integrated Products Team (WIPT) for Milestone B Program Protection requirements; and
- From May 2009 to March 2011 she was a consulting systems engineer for technology protection at Intuitive Research & Technology Corporation in Huntsville, AL, in support of the program protection planning for the IAMD Program Office; and
- From May 2010 to May 2013 she worked through Intuitive at the Precision Fires Missile Systems Alternate Warhead Project Office, in Huntsville, where her duties included identifying critical program information, identifying security and protection requirements to include anti-tamper and information assurance requirements, and providing acquisition documentation input.

Ms. McInnis has never been adversely terminated or suspended from any position in her federal government career, and has received substantial commendations for her engineering work.

6. Relator Tiffany D. Atkins is in the U.S. Army Corps of Engineers, and was the Information Assurance Manager for the United States Department of Defense's Integrated Air and Missile Defense (IAMD) project from the summer of 2010 to May 31, 2013. Since then she has been a project manager for information assurance and IT specialist (INFOSEC) at the U.S. Army Corp of Engineers. Her duties in Information Assurance and as the Information Assurance Manager (IAM) of the IAMD from 2007 to May 2013 included:

Performing Information Assurance Manager (IAM) duties, including:

- Monitor and manage Information Assurance (IA) Controls for a Mission Assurance Category (MAC) I Classified System (tactical) and a MAC II Classified System;
- Enforce Information Assurance (IA) policy, procedures, standards, guidance, and training requirements per Department of Defense (DoD), Army, and other mandatory requirements;
- Monitor potential IA vulnerabilities or risks to the IAMD program;
- Identify IA issues, recommend and implement solutions;
- Voting member of the IAMD Engineering Review Board (ERB) to review and evaluate the effects of IA of system changes;
- Lead for the preparation of IA certification and accreditation documents for Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP);
- Provide security expertise for classified tactical system, verify the security posture of the system before development and testing, advise higher individuals concerning the significant IA changes and the impact to the system, and ensure that IA is addressed in relevant system documentation;
- Review and comment on system scans;
- Develop training of IA controls for IAMD personnel;
- Lead the review to determine, document, and design applicability to IA functions; and
- Update the Army Portfolio Management Solution (APMS) system which coincides with quarterly Federal Information Security Management Act (FISMA) reports.

Preparing detailed plans, budgets, and/or schedules for assigned areas, including:

- Develop and execute a plan for IAMD IA path ahead.
- Lead (responsible for interviewing, writing, and staffing) for 3 IAMD IA Milestone B documents;
- Serving as the Program Analyst to report on Special Project operations, including:
- Monitor and analyze requests for funds for the special project to assure that it is effectively planned and is within overall program cost and schedule;
- Work with the Deputy Product Manager for IBCS Software to develop a preliminary cost estimate for the Director of Program Operations;
- Monitor requests for additional funding by other organizations working on the special project; and
- Update near term activity schedule charts and various plans for the special project.

Coordinating and providing Special Program software tools and IT support, including:

- Lead for a team of government and contractor personnel in the development, updating, validation, verification, and populating of a web based application (S4);
- Consistently review the S4 application to make sure it works properly and troubleshoot problems with the application as they arise;
- Brief Special Project members on the S4 application;
- Continuously train special project members (over 100 individuals) for the S4 application;
- Manage the verification and validation processes in relation to the S4 application; and
- Performed duties as the Deputy Operations Officer of the Special Program, including maintaining physical security at the special project facility, coordinating IT support, and troubleshooting facility and IT issues.

Completing actions for the Annual Management Control Assessment, including:

- Perform duties as the Management Control Administrator and the Internal Control Administrator; and
- Author of the FY08 Annual Statement of Assurance of Internal Controls for the IAMD Project Office.

7. Relator Atkins's last day in her position as Information Assurance Manager at the IAMD Project Office (PO) was May 31, 2013. She left that position to accept a

position for a higher grade and pay promotion from another organization. Her decision was also prompted by negative pressure from the IAMD Project Manager and Deputy Project Manager for her attempts to resist the non-compliance, cover-up and fraud described herein. Ms. Atkins has never been terminated or demoted during her government career, and has been rated excellent.

8. From May 14, 2007, to August 4, 2007, Relator Atkins was an intern analyst with the federal Government Accountability Office (GAO). From September 18, 2005, to May 14, 2007, she was a program analyst for the U.S. Army's Program Executive Office (PEO) Missiles and Space program, in the Lower Tier Project Office (LTPO). From June 2, 2003, to September 17, 2005, she was a student program analyst with the PEO, MS LTPO. Regardless of her title, most of Relator Atkins's duties while working in three different project offices in the PEO-MS program centered on Information Assurance.

9. Relator Atkins's education includes: a December 2012 Master of Science degree in Information Assurance and Security from the University of Alabama in Huntsville; a 2007 degree of Master of Business Administration (MBA) from the University of Alabama in Huntsville, with a concentration in Management of Technology; and a 2005 Bachelor of Science in Business Administration degree, with majors in accounting and management information systems, from the University of Alabama in Huntsville.

III.
JURISDICTION AND VENUE

10. This action arises under the United States False Claims Act, 31 U.S.C. 3729 et seq. This Court has jurisdiction pursuant to 28 U.S.C. §1331 and 31 U.S.C. §3732(a).

11. There was no "public disclosure," as that term is defined in the False Claims Act, 31 U.S.C. §3730(e)(4)(A), of the false claims or allegations herein, prior to the filing of the Complaint.

12. To the extent that the United States has any knowledge of the false claims or statements alleged herein, Relators are "original sources" of that knowledge, as that term is defined in the False Claims Act, 31 U.S.C. §3730(e)(4)(B), based upon their direct and independent knowledge of information upon which the allegations herein are based, which was voluntarily provided to the Government before this Complaint was filed.

13. Venue in the United States District Court for the Southern District of Ohio, Western Division, is proper pursuant to 31 U.S.C. §3732(a) since many of the false claims for payment at issue in this action were submitted to and paid by the Defense Financing and Accounting Service (DFAS) in Columbus, Ohio.

IV.
BACKGROUND

14. In December 2006, the U.S. Army recognized a need to integrate its many battlefield command systems for the operation of radars, launch and guidance systems relative to the number of field deployed missile defense weapon systems.

15. On December 13, 2006, the Army Requirements Oversight Committee approved a capabilities development document requiring the Army to develop and field an Integrated Air and Missile Defense (IAMD) System of Systems (SoS) capability.

16. The need for the IAMD arose from the experiences of the United States military during its operations in the first and second Iraq wars. The Executive Summary of the Contract explains: "The goal of network - centric operations is using the data from any sensor to fire any weapon to defeat threat targets." It would allow air and missile defense

commanders to integrate and work seamlessly with all military units, down to the platoon level, with an integrated fire control network. The contract called for "development of unique hardware and software items that allow the integration of all the weaponry (current and projected) with all the radar, imaging and other sensors into one unified battle command system." In addition to making the U.S. military more effective and defended on the battlefield, a goal of the new IAMD system is to "reduce manpower, enhance training and reduce operation and support cost."

17. The U.S. Army solicited Requests for Proposal (RFP) from interested parties to bid on the system and to provide their concept for the development of the system requirements. A Source Selection Evaluation Board (SSEB) was convened to review and decide on a prime contractor for the effort.

18. Two companies submitted proposals. The SSEB was broken up into two phases using the "rolling down-select method". In Phase 1 of the process, the government awarded two contracts to continue to Phase 2. The result of Phase 2 of the SSEB was to down-select to the current Prime Contractor for IBCS, which is Northrop Grumman.

19. During Phase 1 of the SSEB, the Board was composed of approximately 100 members. While the SSEB is supposed to be a completely independent body free from any and all external pressure when arriving at its conclusion, this did not occur. The Army's Project Manager (PM) of IAMD at that time, Robert Thomas, repeatedly interfered with Phase 1 of the SSEB.

20. The SSEB Chairman of Phase 1 reported PM Thomas for his interference to the Source Selection Authority (SSA). PM Thomas reacted by calling the Chairman to his

office and reprimanding him, and subsequently replaced him with a new SSEB Chairman for Phase 2 of the SSEB.

21. During Phase 2 of the selection process, the new SSEB Chairman often visited PM Thomas, and Thomas's Army team members Deputy Project Manager James Michael (Mike) Achord and Technical Director Jeff Stevens, at the IAMD Project Office (PO). The board location was also moved closer to the IAMD PO offices in Huntsville, Alabama. It was made clear to members of the SSEB that they had to justify any negative assessment of Northrop Grumman and any positive assessments of the other bidding company.

22. Members of the SSEB have made statements subsequent to the selection of Northrop to the effect that if there was a protest to the prime contract obtained by Northrop Grumman that they would not be comfortable testifying to the veracity and integrity of the Board's report. In order to keep the losing company, Raytheon, from protesting the award of the prime contract at Northrop, Raytheon was offered and later awarded a sole source contract, before the protest phase was complete, to provide a portion of the IAMD system.

23. Defendant Northrop Grumman, through its subsidiary Northrop Grumman Space and Mission Systems Corp, located in Huntsville, Alabama, was first awarded a military contract to build a prototype Integrated Air and Missile Defense (IAMD) Battle Command System (IBCS). The effective beginning date of the contract, W31P4Q-08-C-0418, was September 23, 2008. The initiation of Northrop Grumman as the IBCS prime contractor for the next phase, the Engineering and Manufacturing Development (EMD) phase, began in December 2009. The contract expiration date was set for September 30, 2016.

24. The contract included three phases. Phase I is the IBCS Preliminary Design Phase, and is a cost-plus-fix-fee type military contract. Phase II of the contract is the IBCS System Development Demonstration Phase and payment was set as a cost-plus-incentive-fee. Phase III is the Production and Deployment Phase of the IBCS, and payment was set as cost-plus-incentive-fee. Each of the phases provided for many millions of dollars of payment to Defendant for its work. (See Exhibit 1, pages 1-6 of the Contract). For further explanation of phases and milestones of this contract, also see Exhibit 2, a chart depicting the "Weapon System Development Life Cycle."

25. Progress payments are a form of government-furnished interest-free financing available for cost-plus contracts, like Defendant had and has in this matter. On each SF 1443 "Request for Progress Payment" form, Defendant certified to the United States, inter alia, that the work reflected was actually performed. By submitting its periodic request for payments, Defendant certainly represented (expressly and/or implicitly) to the United States Army and government that it was incrementally completing the work it promised to do under the Contract. Such claims by Defendant Northrop Grumman were false because it was not providing valid Anti-Tamper protections, Information Assurance protections and Configuration Management.

26. Computerized, electronic communication of fused information is at the heart of the software and hardware that was to be created by Defendant for the United States military in the new IAMD Battle Command System. The United States military started learning at least with World War I, and over 70 years ago, in World War II, how crucial the security of communications could be to the winning or losing of battles and even an entire war. The importance of safe, secure military communications has grown, not

lessened, since then. Thus, Information Assurance (IA), the general name given to protecting and defending information and information systems (to include weapon systems) from enemy or foreign intrusion, is a crucial, necessary component of the IAMD program product that the United States military is paying Defendant to provide.

27. Likewise, anti-tamper technology (AT) is an absolutely essential component of software and hardware protection in military weapons and systems, especially for prevention of reverse engineering. AT encompasses systems engineering intended to prevent and/or delay exploitation of critical technologies in U.S. weapon systems. AT engineering is essential in the entire life-cycle of systems acquisition, including research, design, development, implementation and testing of AT measures. Properly done AT adds longevity to a critical technology by deterring efforts to reverse engineer, exploit, or development countermeasures against a system or system component. AT is not intended to completely defeat such hostile attempts, but it should discourage exploitation or reverse engineering or make such efforts so time-consuming, difficult and expensive that even if successful, a critical technology will have been replaced by its next-generation version. Attached as Exhibit 3 is a 4 page introduction to Department of Defense (DOD) anti-tamper policy, with pertinent statutory and DOD regulatory policy and guidance.

28. Importantly, IA and AT are not add-on components, but must be fully integrated into the IAMD IBCS software and hardware from inception. The IBCS is in reality about 85% software development. If IA and AT are not properly done, the IAMD IBCS software and hardware fail to meet contract specifications and Defendant has delivered a product with absolutely no value to the government and exposes other key

weapons systems to exploitation.[1] Defendant's delivery of adequate IA and AT are crucial because the system must be deployable in foreign and hostile environments.

V.
NORTHROP'S WRONGFUL CONDUCT

A. Relator McInnis's Knowledge of Fraud

29. Relator McInnis began her involvement with the IAMD program as early as May 2006, when she was a contract consultant with the Army Research & Technology Center that was identifying Critical Program Information (CPI) for the Milestone A Decision[2] of the IAMD. From May 2006 to February 2008, Ms. McInnis, as a certified Technology Protection Engineer, was the lead engineer for the Integrated Product Team (IPT) that performed the following functions for the Army:

- Critical program information assessments;
- Intelligence production requests completion;
- Multi discipline counter intelligence threat assessment evaluation;
- Vulnerability analysis;
- Risk assessments;
- International traffic in arms (ITAR) control technologies evaluation; and
- Countermeasure planning to include cost analyses.

---

[1] It is irrelevant whether the program, without appropriate AT and IA, may have value to purchasers other than the U.S. Government. Relators are aware that Northrop has actively solicited foreign purchasers, and the IAMD program, even without the IA and AT necessary for U.S. military usage, may have significant future commercial value to Northrop. Relators suspect that Northrop may have intended all along to use the IAMD-IBCS contract as a means of getting the U.S. Government to pay the research and development costs of a product that would generate significant future commercial revenue for Northrop.

[2] Milestones are used in the defense acquisition system to oversee and manage acquisition programs. At each milestone, a program must meet specific statutory and regulatory requirements before the program can proceed to the next phase of the acquisition process. There are three milestones:

- Milestone A: initiates technology development,
- Milestone B: initiates engineering and manufacturing development, and
- Milestone C: initiates production and deployment.

The end products of their work by February 2008 included:

- Program Protection Plan (PPP);
- Protection Implementation Plans;
- Security Classification Guides;
- Delegation of Disclosure Letters;
- Technology Assessment/Control Plan;
- System Security Engineering specification requirements;
- Export policy
- International distribution requirements; and
- The contract statement of work (SOW) requirements.

30. In December 2009 Northrop Grumman (NG) began its work on the massive IAMD IBCS contract, as the prime contractor, in the Engineering, Manufacturing and Development phase (EMD).

31. Section 3.2.3.7.5, Section 3.2.3.7.5.1, and Section 3.2.3.7.5.2 in the Contract Statement of Work (SOW) expressly require that Northrop Grumman "shall" develop and implement the Anti-Tamper (AT) Annex to the Program Protection Implementation Plan (PPIP). (The Annex is a classified document.) Also, Section 3.2.3.10.1.5 of the Contract SOW states that a Product Baseline Update Review must include a PPIP with AT Annex with government approval without comments. To approve it with comments would essentially be admitting that the PPIP/AT is inadequate. Furthermore, DoDI 5000.02 mandates that anti-tamper protection is required for systems with Critical Program Information (CPI) and Critical Technologies (CT).

32. Critical Program Information (CPI) consists of components of a research, development and acquisition (RDA) program that, if compromised, could cause significant degradation in military mission effectiveness, shorten the expected combat, effective life of the system, reduce technological advantage, or enable an enemy to defeat, counter, copy, or reverse engineer the technology or capability. As the Defense Acquisition Guidebook advises all military contractors: "Metaphorically, CPI should be thought of as the technological crown jewels of the program." See attached Exhibit 4, which are pertinent excerpts from the Defense Acquisition Guidebook (DAG) describing CPI in more detail, and providing DoD pertinent regulations.

33. From February 2008 to May 2009, Ms. McInnis was away from the IBCS project work while she worked on technology protection with a NASA program. But in June 2009 she began working for IAMD contractor AEgis Technologies Group in Huntsville, AL, as the subject matter expert engineer on technology protection systems for the IAMD program. Her duties were to ensure that program protection tasks were integrated into the systems engineering management, test and evaluation, and program management. She served in this capacity through AEgis until March 2010. From March 2010 to March 2011 she served in that capacity as a consultant through contractor Intuitive Research and Technology Corporation.

34. Northrop's first false claim was in claiming that they could provide the Engineering, Manufacturing and Development (EMD) of the IBCS, in compliance with Department of Defense regulations, and within the contract specifications on cost, schedule and performance. In its proposal for software for the IBCS, NG as a rule stated: "To be determined." This lack of detail demonstrated that NG had failed to perform the necessary

diligence and preparation to enter into the EMD phase of the contract. Based upon her education, training and experience, Ms. McInnis knew that NG had not done sufficient program protection planning to include anti-tamper planning. This was abundantly clear to Relator McInnis in the late summer of 2009 at the Preliminary Design Review (PDR). The purpose of the PDR in the Weapon System Development Life Cycle, as a necessary step for Milestone B, is to verify and validate to the military that you, the contractor, have worked on and prepared a valid design with sufficient anti-tamper (AT) protections, Information Assurance (IA) protection and Configuration Management among other necessities. Relator McInnis, and Relator Atkins, could see that Defendant NG had simply not done this.

35. On August 11, 2009, an Army IAMD team led by Charley Robinson, the Army's IAMD PO Systems Engineering Director, received a briefing, at his request, from Relator McInnis, to provide his team with an understanding of Anti-Tamper (AT) requirements and the processes for meeting such requirements.

36. Relator McInnis, along with Relator Atkins, were members of the Army Integrated Air and Missile Defense System of Systems (ASoS) Program Protection Working Integrated Products Team (PP WIPT). This team was established under authority of DoD Instruction 5000.02, Operation of the Defense Acquisition System, DoD Instruction 5200.39, Critical Program Information (CPI) Protection within the Department of Defense, DoD 5200.1M, Acquisition Systems Protection Program, along with other DoD memorandum. The mission of the PP WIPT is to "develop and implement a Program Protection Plan (PPP)," based on "identifying critical technologies, systems, or information that are designated as the program's CPI and to safeguard DoD information and

technology from unauthorized disclosure to foreign interests." The PP WIPT was primarily made up of Army civilian personnel, like Relator Atkins, as well as contractor personnel like Relator McInnis. Around 40 people were on the WIPT, including:

- Chair Jeff Stevens, the Army's Technical Director (TD);
- Mike Achord, the Deputy Project Manager (DPM) for the IAMD project.
- Co-Chair Kelli Smith, the International Office Director for the Army on the IAMD project;
- Charley Robinson, the Army's System's Engineering Director for the IAMD project;
- Dr. Robert Overbeek, the Anti-Tamper Engineer from the Army's Aviation Missile Research Development Engineering Center (ARMDEC);
- Tiffany Atkins, IAMD's Information Assurance Officer; and
- Patricia McInnis, Contractor Support, and identified as part of the Leadership of the PP WIPT.

37. In September 2009 NG participated in identifying Critical Program Information (CPI) for its IBCS design, with the PP WIPT. Based upon NG's proposed design, four CPIs were identified, along with one other possible CPI for the Milestone B decision. This CPI assessment was a crucial component for determining whether the program plans were affordable and executable, and whether the program was ready to proceed to the Engineering, Manufacturing and Development (EMD) phase.

38. It is significant that no CPI had been identified prior to September 2009. October 2009 was the time for the milestone decision for the IBCS project to proceed into the EMD phase. The lack of any identification of CPI at that time in September 2009

demonstrated to Relator McInnis and others on the PP WIPT that NG failed to develop the necessary understanding of the criticality and consequences of AT and IA protection requirements. Relators firmly believe that an EMD contract should never have been awarded to NG.

39. As a prime contractor, NG had and has a responsibility to know all applicable Department of Defense (DOD) regulations and concomitant policies. If a system contains Critical Program Information (CPI) and Critical Technology (CT), then Anti-Tamper (AT) technology is required to protect the CPI and CT from exploitation, according to federal regulations DoDD 5000.1 and DoDI 5000.2. DoDI 5200.39 contains the instructions for protecting CPI.

40. Relator McInnis saw in the late summer and autumn of 2009 that NG personnel did not take program protection seriously. After the contract was formally issued in December 2009 and begun in January 2010, Ms. McInnis could see further that NG personnel demonstrated that they did not know, did not understand or did not intend to comply with the Department of Defense regulations and policies for system assurance, protection and security.

41. On September 22, 2009, the CPI Assessment Memorandum (a classified document describing the CPI) was provided to the Defense Information Board (DIB). This is one of the Pentagon offices that assess program protection plans.

42. On November 19, 2009, a Conceptual Anti-Tampering Plan was issued by the PP WIPT. This Plan was created by Relator McInnis and Ms. Kelli Smith, with input from the PP WIPT. The Plan set forth the Anti-Tampering level requirements, actions needed and time frame. Defendant NG failed to deliver these, despite the fact that Relator

McInnis and the PP WIPT provided NG with a detailed template for an AT plan. The template and the Conceptual AT Plan included the need for identifying threats and vulnerabilities, and examining the consequences and risks to system performance, battlefield capabilities and negative economic considerations for the United States and its military industries.

43. Initially Dr. Overbeek, the technical representative of the Army's AT Group at the Anti-Tamper Agency, approved the Conceptual Anti-Tamper Plan with reservations, to allow the Milestone B program protection plan requirement to ostensibly be met and the project to proceed. However, he later clearly communicated its inadequacy via an **e-mail of May 7, 2010. See Exhibit 5.** To the best of Relators' knowledge, Dr. Overbeek and the Anti-Tamper Agency have never approved any required Anti-Tampering Plan for Defendant NG.

44. In November 2009, and repeatedly thereafter, in technical interchange meetings, Relator McInnis stressed the need for threat trees to Army and Defendant NG personnel, including NG's David Beals, Sam Hawkins, Greg Lazarian and others. Threat trees are an essential component in the industry for identifying threats, vulnerabilities (the likelihood that a weakness or susceptibility will be exploited by an adversary) and consequences of the exploitation. Even when Relator McInnis resigned from the IAMD work nearly a year and a half later on March 31, 2011, no adequate level of threat trees had been completed. Professionals in the industry like her know that anti-tamper protection cannot be adequately designed into a system if the threats are not adequately analyzed. The concerns and warnings expressed by Relator McInnis to NG and the Army's Project Manager (PM) and Deputy Project Manager (DPM) were joined by Dr. Overbeek and

Kelli Smith. In addition, NG's Greg Lazarian concurred in their assessment and warnings. As a result, Mr. Lazarian was removed from his position.

45. As explained in the Defense Acquisition Guidebook, any major weapon system development must have an Acquisition Strategy, an Acquisition Plan, and an Acquisition Decision Memorandum. For the IAMD IBCS program, the 2009 Acquisition Strategy, the Acquisition Plan and the December 2009 Acquisition Decision Memorandum all referred to Foreign Military Sales (FMS) and contemplated those sales as an important part of this program. Based upon Relators' experience and training in the military industry, any development of a weapon system is done with the assumption that FMS are contemplated. A Technology Assessment/Control Plan is also required when there is to be any foreign involvement with a weapon system. Relator McInnis, Kelli Smith, the Army's international specialist for this program, along with other members of the PP WIPT started developing a Technology Assessment/Control Plan. In addition, a Delegation of Disclosure Letter is only required if there is to be foreign participation in a program.

46. The Defense Acquisition Guidebook is a compilation of U.S. defense statutes, regulations, policies and best practices for acquiring new systems. See dag.dau.mil. Defendant NG was well aware of this guidebook.

47. On January 19-22, 2010, a contract kick-off meeting was held. The purpose was to lay a solid foundation for a mutual understanding of the project risks. Participants included NG personnel, including David Beals, its lead engineer, Sam Hawkins, its systems engineer, Greg Lazarian and others, along with key government officials. Mr. Lazarian was NG's systems engineer with a background in anti-tamper, but Sam Hawkins's background was in psychology. Mr. Lazarian was subsequently removed from

his position in the spring of 2010, despite the fact that the government was suppose to approve personnel changes. (See Section H-16 on "key personnel" in the contract). At this kick-off meeting, Relator McInnis was surprised when NG did not address anti-tamper as a risk element, so after awhile she openly addressed it. "Anti-Tamper has not been addressed during this kickoff meeting, and I recommend that anti-tamper be added to the Action Items List." Relator McInnis was shocked to realize that NG's David Beals was making an effort to ignore her. She persisted, so Beals told the group that he would add it to the action item list. However, anti-tamper never was placed on the "action item list," and NG never had anti-tamper in their risk management plan. The repeated warnings by Relator McInnis and Kelli Smith were ignored. Relator McInnis had the distinct impression that the involved NG personnel and the Army's PM and DPM were incompetently ignoring AT program protection.

48. Relator McInnis could see in January 2010 that Northrop Grumman knew that they could not provide AT protection, but kept acting and claiming as if they could. This was fraud, when they were collecting millions of dollars on that premise. To the best of Relator's McInnis's knowledge, NG has still (1) not developed adequate anti-tamper technology, (2) cannot implement it and (3) keeps taking millions of taxpayer dollars.

49. On January 23, 2010, a draft Delegation of Disclosure Letter (DDL) was issued by Kelli Smith, and it was given to Mike Achord, the Deputy Project Program Manager (DPM), and to the Army's G2 intelligence unit. Relator McInnis heard nothing more about this during her time working on the IBCS. The DDL specifies what information can be released to foreign nationals, and what cannot. It is necessary for any foreign military sales (FMS) involvement. Everything Relator McInnis and Relator Atkins

saw of the IAMD-IBCS program from 2006 into 2010 indicated that it was to be a program with foreign participation, and not a U.S.-Only system.

50. The anti-tamper technology requirements for a U.S.-Only system are much less than the AT requirements for foreign military sales (FMS) or International Cooperation. Unsurprisingly, the exposure level of critical program information and critical technologies (CPI/CT) is much greater for FMS and international cooperation. Thus, the anti-tamper requirements are much more extensive and expensive where the program will involve FMS and international cooperation. However, even where weapons or systems are U.S.-Only, anti-tampering requirements are still necessary because of theft within the U.S. and the likelihood of battle field losses of such equipment with the attendant risk of reverse engineering.

51. On February 12, 2010, Relator McInnis and Kelli Smith of the IBCS program office met with Dr. Robert Overbeek, the Anti-Tamper Engineer of the DOD Anti-Tamper Agency. They discussed the risk of a U.S. adversary exploiting the weaknesses or susceptibilities of virtual machines, and the means of protecting against exploitation. The submitted Milestone B Conceptual AT Plan, an Annex to the Milestone B Program Protection Plan (PPP), stated that NG's anti-tamper plan was to be provided to the government within 30 days of the contract award in December 2009. Not only was it not provided by February 2010, it had still not been produced by Defendant NG, as an AT design verified by the Anti-Tamper Agency and Dr. Overbeek, as of April 1, 2011, when Relator McInnis left the IAMD program. To the best of Relators' knowledge it still has not been verified and approved by Dr. Overbeek and the Anti-Tamper Agency.

52. In a February 18, 2010 meeting, Relator McInnis and the PP WIPT identified anti-tamper level requirements for 11 IBCS components where CPI resided. AT levels characterize what technology is to be used to minimize exploitation and reverse engineering. For example, one level might require hermetic seals, and another level may require trusted processors and encryption. Present were Relators McInnis and Atkins, NG's Beals, Hawkins and Lazarian, and officials from the Army IAMD program Office (PO), including Charlie Robinson, Jeff Stevens and Kelli Smith. Relator McInnis and Kelli Smith identified 11 hardware end items where at least four areas of Critical Program Information (CPI) resided on the IBCS system, and thus were Critical Technologies (CT), requiring AT technology for protection. This meeting occurred at the IBCS Program Office (PO).

53. The Contracts Data Requirements Lists (CDRLs) are required contract documentation deliverables for NG. While NG delivered alleged CDRLs, the anti-tamper components, CDRL A035, were never approved by the PP WIPT which included Dr. Overbeek, Relator McInnis, Kelli Smith, Relator Atkins and others. Despite this failure of approval, PM Thomas later approved the CDRLs "with comments." While this approval with comments by PM Thomas allowed for NG to keep collecting millions of dollars, it could not change the fact that NG was failing to fulfill the necessary work of the contract on anti-tamper, and NG unquestionably knew this.

54. In March 2010 Defendant Northrop Grumman submitted its Program Protection Implementation Plan (PPIP) with a deficient anti-tamper plan, despite the legal requirements and the advisories and warnings described above. Not surprisingly, the

Contracts Requirements Data List (CDRL) A035 of the contract was rejected by the Army's PP WIPT.

55. The Tri-Services Committee is a Department of Defense Group for the Army, Navy and Air Force. Its mission centers on DoDI S-230.28, a secret regulation that identifies technologies that must be protected. The Committee is comprised of Colonel-level officers of the Army, Navy and Air Force, and it meets regularly to assess system protection solutions, so that military critical technologies will not be exploited by United States adversaries resulting in loss of combat effectiveness, or economic losses.

56. In March 2010, the Tri-Services Committee began an assessment of what NG had produced for levels of protection relating to foreign involvement. NG realized that they could never meet these levels of protection. Retired Colonel Ron Jassey, NG's Program Manager for the IAMD IBCS contract, admitted around this time: **"We'll never pass Tri-Services."** This is based upon Relator Atkin's belief and information from other Army co-workers. Thus, Defendant NG had knowledge of its failure to obey the IAMD IBCS contract but continued and continues to accept millions of dollars.

57. The Tri-Services Committee's assessment was communicated to the IBCS Program Office in May 2010. This is when Program Manager Thomas, undoubtedly at NG's urging, started declaring that the IBCS was a "U.S.-Only system." However, based on information and belief of Relators, after May 2010 NG officials, DPM Achord and Jeff Stevens of the PO Office held meetings with foreign nationals in which they briefed them on the IBCS system.

58. On April 7, 2010, a briefing occurred between Northrop Grumman's Beals, Hawkins and others, with DPM Achord and Kelli Smith of the IBCS PO, and Relators

McInnis and Atkins, over concerns for the Information Assurance (IA) and Program Protection (PP) for the Plug and Fight (PnF) Kit, commonly referred to as the B-Kit. The necessary threat/vulnerability/risk assessment was not complete, the use cases were not complete, and the horizontal protection requirements were not understood for the B-Kit. It was clear that Defendant NG personnel failed to understand the anti-tamper requirements. NG's Greg Lazarian had been removed from his position around this time.

59. On April 28, 2010, a System Security Engineering Tiger Team kick-off meeting was held. Present were Relators McInnis and Atkins, along with Kelli Smith and Charlie Robinson, the Army's IAMD Systems Engineering Director, and Defendant NG's Beals, Hawkins and others. It was again clear to Relators at this meeting that project protection requirements had not been met. Defendant NG was building B-Kit subassembly prototypes without addressing anti-tamper requirements. NG had a subcontractor involved for this sub assembly, which involved a higher risk for AT. There was no validation of proposed countermeasures to protect the B-Kit from exploitation by enemies.

60. At a meeting of May 2010, the Tri-Services Committee tiger team provided its negative assessment of NG's work. As a result, Program Manager Thomas, undoubtedly at NG's urging, started branding the IBCS project as a U.S.-Only system. Based on Relators' information and belief, Mr. Thomas did this in statements and e-mails. The Anti-Tamper (AT) requirement level for a U.S.-Only system is generally lower because the exposure levels are different. Nevertheless, there still remains an anti-tamper requirement. Critical technologies could still be obtained by enemies and exploited.

61. By May 2010, only identification of the IBCS critical technologies had been completed. NG had failed to identify the threats, vulnerabilities, attack scenarios, impacts

if exploited, needed exploitation time lines, available anti-tamper techniques, and it had not selected potential implementations. According to DOD anti-tamper process, NG was supposed to have provided this by Milestone B, in November or at least December 2009.

62. On May 7, 2010, Dr. Robert Overbeek wrote a blunt e-mail to Kelli W. Smith, the Army's international specialist, and the co-chair of the PPWG, criticizing the failure of NG ("the contractor") to "even come close" to meeting the anti-tampering requirements for the IBCS design. See this May 7, 2010, e-mail attached as **Exhibit** 5.

63. At a briefing in early spring of 2010, PM Thomas and Defendant NG's Beals and Jassey told Army officials, including representatives from the Office of Secretary of Defense (OSD) that the IBCS development was on track, and the risks were acceptable, when they knew that NG's system was not fulfilling the contract.

64. On May 18, 2010, a "Way Ahead" briefing occurred at Northrop Grumman offices. Present on behalf of NG were Beals and Jassey. Also present were Relators McInnis and Atkins, with Kelli Smith, Dr. Overbeek and Jeff Stevens, Technical Director of the PO. DPM Achord was also present. The purpose of this meeting was to reassess CPI and what level of protections were needed if it was a U.S.-Only system. Dr. Overbeek made it clear that even if it was a U.S.-Only system, an entirely new mission, that it was still necessary to identify the AT and IA requirements. For example, as an integrated component, what does the Patriot missile require? The NG personnel present continued their seeming indifference to the security requirements. This continued indifference was also exhibited by DPM Achord.

65. By this time period of mid-2010, when the Army's Project Manager and Deputy Project Manager and NG personnel are stating that the IBCS project is to be a U.S.-Only project, they are in fact communicating with foreign nationals about the project.

66. DPM Achord was personal friends with retired Army Colonel Ron Jassey, the Program Manager for Northrop Grumman on the IBCS contract. Mr. Achord told Relator McInnis in May 2009, the first time she met him, that he was close to retirement and hoped to work for a contractor.

67. In September 2010, Relator McInnis worked with a Dr. Peterson on the Raytheon A-Kit protection requirements. Dr. Peterson had led the effort of Raytheon in identifying CPI and the protections needed in the A-Kit. In stark contrast to Defendant NG, Dr. Peterson and Raytheon clearly understood and provided AT requirements.

68. During a review of CDRL A035 in September 2010, by Relator McInnis and others on the PP WIPT, it remained obvious that appropriate, valid AT was missing from NG's work product, including no protection measures to detect or deter reverse engineering.

69. In September 2010, Kelli Smith was removed as the co-chair for the PP WIPT, and replaced with Mr. Mike Maddox. Relator McInnis could see that Mr. Maddox, a newly hired employee for the IAMD Army Program Office's Systems Engineering Division, did not know government policies and regulations for program protection planning. Relator McInnis formed the impression that this new hire was a "tool" for the Army's Project Manager and Deputy Project Manager to relax the requirements to allow NG to continue collecting payments while failing to deliver AT and other protections.

70. At a meeting of the PP WIPT on December 17, 2010, to address anti-tamper, PM Thomas told Mr. Beals of NG to have an anti-tamper plan no later than mid-January 2011. Mr. Thomas told this to Mr. Beals because of the consistent pressure from Ms. McInnis and Kelli Smith on the lack of anti-tamper protections work. Beals quietly responded that he was not sure it was possible with the current IBCS design. Relator McInnis witnessed this further admission of Defendant NG. Mr Beals was correct as NG has never produced a validated AT plan.

71. Thus, NG's Jassey admitted failure and knowledge in March 2010, and NG's Beals admitted the same in December 2010. Further admission and demonstration of knowledge lies in the fact that NG undoubtedly urged the Army's PM and DPM to attempt changing the program to a U.S.-Only system, essentially dumbing it down, in the hope of continuing the contract without adequate AT and IT. Relators firmly believe that the NG program should have been terminated in 2010 at the latest, and started over with a design that would include valid AT, IA and Configuration Management.

72. In March 2011, the federal Government Accountability Office issued a report entitled *Defense Acquisitions: Assessments of Selected Weapon Programs*. It reported, inter alia, that the IAMD program's costs had risen by nearly $600 million since its start. In response to this alarming report, Northrop's IBCS Program Director, Robert Jassey publicly claimed that the reason for the increased costs were the government's fault for including systems like the Patriot that were not originally intended. See May 15, 2013, article from *Inside Missile Defense*, attached as Exhibit 6. This constitutes a part of the cover-up deception by Northrop of the federal government because at least part of its costs

overruns are due to its continual failure to develop valid AT, IT and Configuration Management in the program.

73. In early January 2011, the Contract Data Requirement List (CDRL) for the Program Protection Implementation Plan (PPIP) was resubmitted by NG for review and acceptance by the IBCS program office. The necessary CDRL A035 was woefully deficient for an anti-tamper plan, based upon the review by Dr. Overbeek, Relator McInnis and the PP WIPT. Defendant Northrop failed to deliver as required even as they planned for the Critical Design Review in support of the Milestone C decision.

74. In February 2011 Relator McInnis provided information for an anti-tamper status briefing to Brig. General Ollie Knudson, the Program Executive Officer for the Army's Missile and Space office. Despite Relator McInnis describing the dire state of affairs to Thomas, Achord, Maddox and Robinson, these warnings were not included by them in the briefing to Brig. General Knudson. Relator McInnis was not in the briefing, but she saw the briefing charts that they presented to Brig. General Knudson. It was very clear to Relator McInnis that Thomas, Achord, Maddox and Robinson were painting a rosy but deceptive picture of the AT product to Brig. General Knudson.

75. It was abundantly clear to Relator McInnis at this point in early 2011 that PM Thomas and DPM Achord, in close collusion with NG's Beals, Jassey and others, were desperate to have lower anti-tamper levels accepted to cover for their deception on performance of the contract. Defendant Northrop Grumman's design used virtual machines that could run several different operating systems, and used open system architecture. This made valid anti-tampering protections that much more critical. It was too easy for an adversary to enter such an open system.

76. In March 2011 Relator McInnis resigned, as she no longer wanted to be a party to such inadequate, dangerous anti-tamper technology on a military system. Her efforts were clearly being ignored by NG and the Army PO officials.

77. The Conceptual Anti-Tamper Plan provided to the Milestone Decision Authority (MDA) by the IBCS Program Office in support of the Milestone B Decision identified the most probable anti-tamper requirement, and the time frame for an initial anti-tamper plan. Despite this, NG failed to follow the Conceptual Anti-Tamper Plan and failed to deliver an acceptable Program Production Implementation Plan (PPIP) CDRL.

78. Also, NG's Greg Lazarian was relieved of his PPWG point person duties in the spring of 2010, and replaced by two individuals without any background in program protection and anti-tamper technology. Their background was photography and psychology, without any DOD systems acquisition or systems engineering certifications. Relators believe this constitutes failure to provide qualified personnel to support the contract. Section H-16 of the contract specifies:

> KEY PERSONNEL
> The contractor shall make no key personnel substitutions without obtaining prior Government approval during the first 24 months following the exercise of Clin 0006. Key personnel are identified in the contractor's proposal that resulted in award of this contract. All requests for key personnel changes, along with written justification, shall be submitted to the Contracting Officer.

79. Defendant Northrop Grumman's lack of program protection progress and accomplishment is also exemplified by its lack of performing the Contract SOW requirement of semi-annual Program Protection Surveys. Part 3.2.3.7.5 on Program Protection of the Contract mandates:

> The contractor shall develop and implement an IBCS Program Protection Implementation Plan (PPIP) (CDRLA035) IAW

> DI-ADMN-81306. The contractor shall develop and implement an IBCS Anti-Tamper Annex to the PPIP. The contractor shall support semi-annual Program Protection Surveys.

80. There was substantial effort by the Army and its contractors to assist NG and push it to do things right. Relator McInnis, Kelli Smith, Dr. Overbeek, the Army Anti-Tamper Technical Lead for the Anti-Tamper Executive Agency, and his personnel spent many hours providing guidance and support on anti-tamper program protection planning. Instead of fulfilling the contract and providing anti-tamper security correctly, NG convinced Program Manager Robert Thomas to attempt to fundamentally change the program by declaring in May 2010 that the IBCS was a U.S.-Only system. Mr. Thomas did not have the authority to change the Acquisition Decision Memorandum that was signed by the Milestone Decision Authority (MDA).

81. The Selected Acquisition Report issued on May 21, 2013, which reported on the status of the IAMD program as of December 31, 2012, reported that NG was behind schedule on the IAMD IBCS, and it represented "a four month slip to Milestone C."It reported that NG had not met the contract cost, schedule or performance.

82. Defendant NG failed to follow the security policies and procedures found at http://www.acq.osd.mil/se/docs/acq-security-policy-tool/index.html, including Anti-Tamper (AT) and Information Assurance (IA) protections, and Configuration Management.

83. Thus, in March 2013, Defendant NG, with the cooperation of Project Manager Colonel Robert Rasch, Jr, moved to have the Program Office restructure and rebase-line the IBCS program to essentially dumb it down.

84. Defendant NG's IAMD IBCS contract with the government mandates at part H-1 as follows:

> No change in the scope or within the scope of this contract which would affect a change in any term or provision of this contract shall be made except by a modification executed by the Contracting Officer. The contractor is responsible to insure that all contractor personnel are knowledgeable and cognizant of this contract provision. Changes to contract effort accepted and performed by contractor personnel outside of the contract without specific authorization of the Contracting Officer shall be the responsibility of the contractor.

85. Based upon Relators' information and belief, as recently as February 2014, the Tri-Services Committee asked DPM Achord whether the Anti-Tamper Protection had been completed, and he admitted it had not. Mr. Achord also tried to downplay the extent of the CPI, but eventually admitted the truth of it, including the fact of Sensor Tasking and Data Fusion. Both of these elements are very important as protected critical technologies. Achord could not answer the Tri-Services representative's questions about how such CPI was being protected.

86. The final Anti-Tamper (AT) design should have been completed by the Critical Design Review, and it was not.

87. Defendant Northrop Grumman's false representations that they would provide a combat effective system in accordance with DOD regulations, security policies and procedures, and its false claims that they have been providing such, have cost the American taxpayers millions of dollars, as well as exposing United States Military Systems to exploitation by enemies. At a point four years into the IBCS contract, Defendant Northrop Grumman has yet to demonstrate that they can provide the IBCS with its full requirements for anti-tamper protections.

B. **Relator Atkins's Knowledge of Fraud**

88. Relator Tiffany Atkins believes that for over four years Northrop Grumman has been claiming and taking hundreds of millions of dollars under the IAMD contract, while failing to produce proper, secure Information Assurance (IA). Relator Atkins and her co-workers could see that approximately 70% or more of Northrop Grumman's contract deliverables were rejectable, in the areas of IA, software, systems engineering and others. Northrop Grumman has been able to fraudulently cover up this failure, with the collusion of the Army's former IAMD Project Manager (PM) Thomas and Deputy Project Manager (DPM) Achord in the PEO Missile and Space IAMD Project Office.

89. In March 2010, Relator Atkins and her co-workers rejected numerous contract deliverables (CDRLs) for non-compliance with IA, software and systems engineering specifications. However, her supervisor, DPM Achord, overrode their objections, changing the assessments from rejected to "accepted with comments." The result of this cover-up was that the technical security specifications for IA and other areas were never fixed. The overriding of these objections was done with the knowledge of Northrop and under the direction of Robert Thomas, the IAMD Project Manager (PM) at that time in March 2010. Thomas made it clear to the Directors and Product Managers of the IAMD Project office that CDRLs from NG were not to be rejected thereafter, and the Directors and Project Managers ensured that Relator Atkins and her co-workers were aware of this new "policy." On at least three occasions after April 2010, DPM Achord countermanded Relator Atkins's critical comments on reviews of Northrop's IA work product and instructed Relator Atkins to brand them as acceptable. Relator Atkins refused,

and she was either overridden or NG was allowed to pull the document without receiving the rejection designation.

90. In November 2010, the United States Government Accountability Office (GAO) conducted an assessment of the IAMD program. It was part of the GAO's Ninth annual assessment of DoD weapon system acquisitions, "an area that is on GAO's high-risk list." In its report of March 2011, the GAO stated this about the IAMD program, as of November 2010:

> **"However, according to program officials, the technologies will not be fully mature until after the design review in August 2011. As a result, the program will not have demonstrated that the proposed design meets requirements until after the design review, which puts it at risk for late design changes."**

Under "Technology Maturity" in the report, the GAO reported:

> **In August 2009, the Office of the Deputy Assistant Secretary of the Army for Research and Technology approved a technology readiness assessment that stated that all of the critical technologies were tested in a relevant environment using digital simulations . . . Program officials estimate that the technologies will be mature by the IAMD production decision in 2014, but not by its planned August 2011 design review."**

The GAO also reported that "the Army stated that the IAMD program entered the engineering and manufacturing development (EMD) phase in December 2009 after a competition prototyping phase lasting 15 months. During this phase, the competitors (Raytheon and Northrop) developed IBCS prototypes which were demonstrated to the government prior to the selection of one contractor (Northrop). Both contractors were assessed at technology readiness levels necessary for entry into the EMD phase. Subsequently, Northrop's design was re-assessed in December 2010, and all critical technologies were at the level needed for the current phase of the program." The Army

further reported to the GAO that the IAMD system had reached Technology Readiness Level 6, which is defined as:

> High-fidelity lab demonstration or limited/restricted flight demonstration for a relevant environment. Integration of technology is well defined.

However, Relators are keenly aware that "integration of technology" was certainly not well defined for the IAMD program in November 2010 with respect to AT, IA and Configuration Management, and still wasn't by the middle of 2013.

91. In July 2011 Northrop Grumman's William Farnsworth, the chief of its Information Security (IS) section for the IAMD contract, gave a presentation to government IAMD officials called the "IBCS Gate Review." In the presentation, Farnsworth claimed that Northrop Grumman was well aware of the IA requirements, including AR 25-1, AR 25-2, DoD 8500, DoD 8510 DIACAP and others. Mr. Farnsworth also made it clear that NG was aware of the need to have the STIGs and other IA protections incorporated throughout the software development process for the IBCS, and emphasized this with one slide among a number of slides used in his presentation. This is significant because later, especially by the middle of 2013, Farnsworth and NG were trying to "dumb down" the IA requirements, including claiming that the STIGs were simply guidelines, not requirements. This is because Farnsworth and other NG officials, along with PM Rasch, DPM Achord, Relator Atkins and others knew that NG could not fulfill the requirements.

92. A STIG is a Security Technical Implementation Guide. STIGs consist of a compendium of DOD policies, security regulations and best practices for securing Information Assurance, and Information Security. They are mandated by DODD 8500.1 and 8500.2, and endorsed by CJCSI 6510.01, AFI33-202 and AR 25-2. The goal of STIGs

is to provide a secure configuration for hardware and software to avoid intrusion or detection by foreign militaries, governments or any other unauthorized persons. They also contain technical information to "lock down" information systems or software so that they avoid malicious computer attack. IAVMs are Information Assurance Vulnerability Management programs. Northrop Grumman claimed to the Army that it was incorporating this IA into the design and development of the IAMD IBCS system, but it was not.

93. In 2012, Project Manager Colonel Rasch in desperation sent three members of a separate contractor, Dynetics, to Northrop Grumman in an attempt to fix its algorithm deficiencies. Despite this effort by another contractor, the March 2013 rejection at G-SIL emphasized Northrop's failure to perform the requirements of the contract. The Army paid this contractor for work that Northrop had already been paid to perform.

94. In September 2012, Relator Atkins confronted DPM Achord about what she clearly saw as Mr. Achord's letting NG evade its requirements on IA. She forced him to admit, via an e-mail of September 27, 2012 that there was a "gentleman's agreement" occurring. See attached Exhibit 7 for the September 21 and September 27, 2012, e-mails between Relator Atkins and Mr. Achord.

95. On November 26, 2012, the Army's IAMD IBCS Program Executive Office sent a letter to Defendant NG rejecting NG's AO33 plan for IA. On that same day of November 26, 2012, Relator Atkins e-mailed DPM Achord advising him of her rejection, and reminding him that she had "been expressing my concerns all along, but I understand that the front office has the authority to override my rejection recommendation, . . ." The next day, November 27, 2012, DPM Achord responded via e-mail to Relator Atkins, making it again clear to her that there were not to be rejections of NG deliverables

under the contract, and expressing his obvious displeasure. Relator Atkins responded to Achord by e-mail on that same day of November 27, explaining why she did the rejection and some of the history of her efforts to have NG meet the IA requirements. Nevertheless, as with past occasions, Achord forced Relator Atkins to change the rejection letter of November 26 to an acceptance with comments letter of November 27, 2012. See attached Exhibit 8 for the November 26 and 27, 2012 letters and the November 26 and 27, 2012, e-mails between Relator Atkins and DPM Achord.

96. In December 2012, Relator Atkins's IA team scanned the Northrop Grumman system to determine its IA security posture for an upcoming demonstration scheduled for October and November 2013. What they found was an IA disaster, with numerous security vulnerabilities. It was as if Northrop Grumman had just pulled the hardware and software out of a box from a retail store just before Relator Atkins's Army IA team showed up. The IA team provided its findings and analysis to Northrop Grumman for it to resolve.

97. Despite having three and a half prior years to do the job right, and additional months after the IA team's findings in March 2013, Northrop Grumman was denied access to the G-SIL (Government System Integration Lab) network by the Army's Software Engineering Directorate (SED), when NG attempted to connect to the ACI (AMRDEC Classified Infrastructure). There were far too many category (CAT) I and CAT II Information Assurance deficiencies on Northrop Grumman's system to allow connection to a government network. This was consistent with the failure of specifications that Relator Atkins and her IA team previously discovered. This March 2013 rejection of

Northrop Grumman's attempt to connect to the G-SIL was not a surprise to Relator Atkins; she expected it.

98. Attached as Exhibit 9 is a series of 10 e-mails from March 20 to March 23, 2013, which demonstrate Northrop Grumman's effort to ram through invalid or non-existent IA protections, the rejected efforts by Relator Atkins to address the failures, and the ostensible ignorance of the Army's Project Manager Rasch about the situation. These communications occurred on the heels of NG's product being rejected by the military's G-SIL laboratory. (Note that "SW" in the e-mails is an abbreviation for software.) It is abundantly clear that NG, via its chief of Information Security William (Bill) Farnsworth, knowingly failed or refused to build in valid Information Assurance, and continues the effort to have our military accept this situation on an oral promise that it will be done later. Retired Colonel Robert Jassey, NG's point man for IS on the IAMD program, essentially tried to convince the Army's PM Rasch not to worry, as it will all be taken care of with "patches." He then immediately blames an "engineering drop" for the problem, and pointedly tells PM Rasch: "There was a meeting this afternoon at Dynetics [another contractor] with all involved that Tiffany supposedly (sic) to get everyone on the same sheet of music and reconcile the differences . . ." In other words, something should be done about Relator Atkins, who is refusing to go along with the failure and cover-up.

99. Just over a week later, during an April 3, 2013, meeting, the G-SIL personnel told all present, including DPM Achord that the IBCS could not connect to the ACI government network. In that meeting, DPM Achord became dismissive and hotly announced that because the PM had just told the Honorable Ms. Heidi Shyu that the system will be in the G-SIL and up and running, they were going to put the system in the

G-SIL and turn it on no matter what! The DPM also stated that "the Colonel" (Project Manager Colonel Robert Rasch, Jr.) was going to be able to go back and tell the Honorable Ms. Shyu that the system was in the G-SIL and turned on. Achord was clearly telling the G-SIL personnel, Relator Atkins and others to act like the security protections were valid and in place when that was not true.

100. The Honorable Heidi Shyu is the Assistant Secretary of the Army (Acquisition Logistics & Technology) and the Army Acquisition Executive (AAE).

101. On April 3, 2013, Relator Atkins provided an e-mail to DPM Achord where she reminded him of the history of NG's IA problems that needed fixing at least since November 2010, along with an e-mail by Farnsworth of NG of September 16, 2011 that demonstrated NG's awareness of the legally required IA. Relator Atkins tells DPM Achord that NG **"knew these IA problems were there in 2010 and they did nothing to fix them. This whole train wreck could have been avoided."** See attached Exhibit 10.

102. On April 9, 2013, Relator Atkins gave a briefing to Project Manager Rasch because Northrop Grumman was claiming that the STIGs on IA were not mandatory but merely guides. Attached as Exhibit 11 are slides from Relator Atkins presentation. They included slides from the Defense Information Systems Agency of July 2010, among others. Even though she had been insisting to PM Rasch, DPM Achord and NG officials for over two years about the importance and mandatory nature of IA requirements, Ms. Atkins sensed she had to do it again. In the presentation, she also provided PM Rasch with four slides from the Northrop Grumman presentation by Mr. Farnsworth back in July 2011, where NG made it clear that it understood the necessity of building in IA protections throughout the project development.

103. In April 2013 Relator Atkins again clearly informed Bill Farnsworth of NG, DPM Achord and other contractors that she was recommending rejection of CDRL AO33 on IA, along with reasons why. This was done in an e-mail on April 4, 2013, along with a follow-up e-mail with more specific comments by Relator Atkins on April 17, 2013. On April 25, 2013, Relator Atkins followed with another e-mail to Farnsworth of NG advising him that DPM Achord agreed with her about rejection on two items in a meeting that day, and pointedly advised Mr. Farnsworth: "This does not indicate that the other critical and substantive comments won't warrant a rejection if not fixed as well." This was followed by DPM Achord informing Ms. Atkins: "What Northrop is asking for is for us to supply them the critical comments that we internally agree to and they will withdraw the document and resubmit. This would start the clock all over again." This is just one instance of DPM Achord's avoiding blatant rejections of NG's deliverables on IA. This clear message to Relator Atkins was followed by Achord meeting with Atkins and trying to verbally get her to change her critical comments.

104. On April 26, 2013, Relator Atkins sent an e-mail to Mr. Farnsworth, NG's Chief of Information Services, DPM Achord, other Army officials and contractor personnel on the IAMD project. She made it clear that the STIGs for IA did not simply mean "guidance" and were not a "Tiffany requirement." Instead, they were requirements of the Department of Defense and the Department of the Army. See attached Exhibit 12 for Relator Atkins's 4-26-13 e-mail.

105. On May 1, 2013, Relator Atkins sent an e-mail concerning the A033 Certification and Accreditation Plan CDRL on IA to Army and contractor personnel on the

IAMD, which directed them to the specific clauses of the IAMD IBCS Contract Statement Of Work that NG was supposed to fulfill, and clearly had not. See attached Exhibit 13.

106. In addition, the Configuration Management Plan of Northrop Grumman has been rejected twice in a row, with glaring omissions in IA, along with numerous problems with the IBCS software. The Configuration Management Plan is a systems engineering process to establish and maintain consistency in performance and attributes throughout the life of the system. Attached as Exhibit 14 are two slides produced by the Defense Contract Management Agency in April 2013, depicting its findings of non-compliance by Defendant. PM Rasch undertook to suppress these findings. Based upon information and belief, Relator Atkins believes that this was done in collusion with Defendant's personnel.

107. On May 22, 2013, Relator Atkins was in a meeting with Northrop Grumman's Project Manager, its corporate IA person, DPM Achord and other NG and IAMD project officials. The topic of the meeting was the deficient Information Assurance of NG, and how they were going to fix it. DPM Achord suggested that other contractors on the IAMD project, Dynetics and Mitre, could send personnel to NG to perform the necessary work for IA. The following day, Relator Atkins alerted four people at Dynetics of Achord's idea. On May 29, 2013, Donald Folds of Dynetics responded to Relator Atkins via e-mail presenting several reasons why he believed Achord's idea was inappropriate. See attached Exhibit 15, the May 23 and 29 e-mails of Relator Atkins and Donald Folds of Dynetics. It is unclear to Relator Atkins whether these two contractors were made to fix or able to fix the IA of the Northrop Grumman system after she departed the project office. Neither MITRE nor Dynetics are subcontractors for Defendant on the IAMD project, and Relator Atkins firmly believes that our military should not be paying a different contractor

to fix the IA failures in a system that a giant corporation was already paid millions of taxpayer dollars to produce and knowingly had not.

108. During this spring and summer of 2013, Northrop Grumman was undertaking frantic "24/7" efforts to fix the IA failures, self-described as "Hail Mary" plays. Properly secure, functional IA should have been built and integrated into the IAMD-IBCS by Northrop Grumman during the three and a half years when it billed for and collected millions of dollars from the Department of Defense. Based upon Relators' information and belief, these efforts have not been successful.

109. To the best of Relator Atkins's information and belief, the official contracting officer was not truthfully informed about these Northrop failures, and has been misled by a cover-up. Also to the best of Relator Atkins's information and belief, in early 2013 the Honorable Heidi Shyu was deceived and misled by charts on the alleged progress made by Northrop on the IAMD project. This was done with the collusion of at least DPM Achord.

110. Another piece of the cover-up involves Barry J. Pike, Deputy Program Executive Officer, PEO, Missiles & Space, who serves as the Designated Approving Authority (DAA). Mr. Pike was initially unaware of Defendant's failures. However, Mr. Pike very recently claimed that the system is accredited, when it is not. Mr. Pike has done this at the urging of Northrop Grumman, in September 2013, to allow the Defendant's system to be put onto the ACI network in time for a demonstration that was scheduled for early October 2013. However, there has been no review by an official Agent of the Certifying Authority (ACA). Northrop Grumman and its confederates in the Army are trying to bypass this review. Indeed, they are attempting to bypass almost every part of an

actual accreditation to get the system on the ACI network. However, the Army's Chief Information Officer (CIO)/G-6 has not approved this maneuver by Mr. Pike and Northrop Grumman. The IBCS, like any other system, cannot bypass the accreditation process required by the contract and regulations. The IBCS is not properly accredited, and if Mr. Pike or others are claiming that it is, they are engaging in deceit.

111. Despite being paid millions of dollars under the Contract for over four years, the Defendant failed to develop and produce software that has adequate Anti-Tamper protections, Information Assurance (IA) and Configuration Management. The software is essentially useless to the military, because the product delivered will either not be used by the government at all, or it is radically deficient. Northrop Grumman was extremely inept in providing the proper level of security for the IAMD Battle Command System. Use of the software product provided by Defendant as of May 2013 would expose the system much too readily to security compromise.

112. Northrop Grumman is required under the Contract to perform and build Information Assurance (IA) into the Battle Command System. For years, Northrop has been falsely telling the government, and causing the government to believe, that it has been designing and building valid, sufficient, quality security (IA). They have been deceiving the government.

113. Northrop Grumman has been scrambling since March 2013 to try to perform the work that it was paid millions of dollars to do in the previous three years. Its product in mid-2013 was plagued by over 100 CAT Is, IIs and IIIs. CAT Is, IIs and IIIs are the severity categories that are assigned to systems IA weaknesses. They indicate the risk level of the weakness and the amount of urgency for corrective action. To understand the

seriousness of this failure, a MAC I Classified system has 159 IA controls, including those mandated by Department of Defense Regulation 8500.02, along with United States Army IA controls. Based on the DoD Information Assurance Certification and Accreditation Process (DIACAP), a system cannot be granted an Authority to Operate with even one CAT I vulnerability. Northrop having over 100 findings, which include CAT Is, for its system demonstrates that Northrop is not even close to IA compliance. Based upon information and belief, Northrop has been trying to get the more serious CAT Is re-categorized as CAT IIs, so it can bypass the G-SIL Designated Approving Authority at the Army Material Command.

114. Many of the specific IA security specification failures by Northrop are classified information, and Relator Atkins refrains from providing particulars herein for security reasons. Relator Atkins has specific, firsthand knowledge of these IA security failures. It was her job to review and analyze Northrop's work product under the contract to determine if they were meeting IA specifications.

VI.
CONTRACT REQUIREMENTS VIOLATED

115. Northrop is required under the contract to provide functional, secure software for the IAMD. The software must meet requirements on (1) quality, (2) anti-tamper protections, (3) Information Assurance (IA), and (4) Configuration Management.

116. In contract paragraph H-1, the United States government expressly addressed and prohibited any modification of contract terms by technical representatives or managers who were not the Contracting Officer, as provided in SECTION H-SPECIAL CONTRACT REQUIREMENTS:

H-1 TECHNICAL LIAISON AND SURVEILLANCE CLAUSE (USAAMCOM)

Performance by the contractor of the technical aspects of this contract shall be under the cognizance of the Integrated Air and Missile Defense (IAMD) Project Office. All technical liaison with and technical surveillance of the contractor, within the scope of this contract, will be furnished by the IAMD Project Manager, or his authorized representative. Communication of technical matters pertaining to this contract shall be directly between the contractor and the Program Manager Executive Office for Missiles and Space. Integrated Air and Missile Defense Project Office, ATTN: SFAE-MSLS-IAMD, Bldg. 5250 Martin Road, Redstone Arsenal, AL 35898-8000, with a copy of such correspondence to the ACO, PCO, and SFAE-MSLS-IAMD-OP.

The above clause is governed by the following:

No change in the scope or within the scope of this contract which would effect a change in any term or provision of this contract shall be made except by a modification executed by the Contracting Officer. The contractor is responsible to ensure that all contractor personnel are knowledgeable and cognizant of this contract provision. Changes to contract effort accepted and performed by contractor personnel outside of the contract without specific authorization of the Contracting Officer shall be the responsibility of the contractor."

117. Defendant violated the 3.2.2.2.10 Information Assurance Certification and Accreditation Plan and 3.2.3.7.4 Information Assurance requirements of the Statement of Work (SOW) portion of the Contract. Northrop Grumman did not "...implement Information Assurance during the design, development and production of IBCS MEIs..." (Major End Items i.e. the major defense system components, such as Patriot, etc.) The Certification and Accreditation Plan (CAP) required in this section was rejected numerous times by Relator Atkins pursuant to specifications and the rules, but Relator Atkins was often overridden and the document was sent out "accepted with comments" by the IAMD front office.

118. Sections 3.2.2.2.10 and 3.2.3.7.4 also require: "The contractor shall ensure that all products provided to the government or that use or are connected to government

facilities are in compliance with DoD Information Assurance Support Environment [website omitted] and DA (AR 25-1 and 25-2) information assurance requirements in existence 10 days prior to date of use." This means that the contractor should have provided the government an IA compliant system that abided by the IA controls for a MAC I Classified system and by all applicable DISA STIGs 10 days prior to the government wanting to use the system. Northrop Grumman's system was denied access to the government network at the G-SIL because of its inadequate IA posture. As a result, the government schedule had to change and venues had to change because IA was not built into the system.

119. The last part of 3.2.2.2.10 and 3.2.3.7.4 of the contract SOW also mandate: "The contractor shall assess and implement all IAVAs that are applicable." Based on the scan done by Relator Atkins's team in December 2012 and the G-SIL scan in March 2013, it is clear that the IAVAs were not implemented. (See P. 14 of Statement of Work.)

120. Section C-1 of the contract mandates compliance with Attachment 001, the Statement of Work (SOW) and the Systems Specifications, Attachment 002.

121. Section H-3 of the Contract on Engineering Change Proposals, and Requests for Deviations of Waivers, mandates at paragraph 2.d.: "The contractor shall not manufacture items for acceptance by the Government that incorporate a known departure from requirements, unless the Government has approved a RFD." Paragraph 2.e. further mandates: "The contractor shall not submit items for acceptance by the Government that incorporate a known departure from requirements, unless the Government has approved a RFW." (Request for Waiver.) Northrop Grumman knowingly breached this when they provided the government a system that could not get certified and accredited on its own.

Defendant's submission of items for acceptance constitutes a certification (express and/or implied) that the product materially complies with all contract requirements.

122. Section H-11 on "SECURITY REQUIREMENTS" in the Contract requires strict compliance with Department of Defense regulation DD254 to prevent security leaks of information to non-citizens or representatives of foreign interest. In approximately April 2011, Relator Atkins reported Northrop Grumman to her co-workers and her superiors when Northrop Grumman was trying to use a particular foreign device for a very sensitive part of the system. (Details of this incident must be explained in a Classified forum.) Defendant did not comply with export laws. Northrop Grumman was never punished for doing so, and the COTR (Contracting Officer Technical Representative) who had signed the DD254 form at the time, IAMD Technical Director Jeff Stevens, did not report this incident, as required by the DD254 portion of the contract.

123. Section H-12 of the Contract mandates: "The IAMD Project Office approval is required prior to discussion of the IAMD Battle Command System (IBCS) Development Program with visitors or representatives of any other agency. Any visitors to the contractor's facilities shall not be granted access to the data unless they meet the requirements of need to know established by government security regulations." (P. 147 of the Contract.) More than once, Northrop Grumman breached this provision. One particular instance is when Israeli visitors were on their premises.

124. Defendant also breached the H-18 Foreign Participation portion of the contract. (Details must be provided in a Classified environment.)

125. Defendant is not compliant with the Contract's 3.2.2.2.4 Configuration Management Plan and 3.2.3.6 Configuration Management. The Configuration

Management plan was rejected more than once during Relator Atkins's tenure, because Northrop Grumman was not adhering to proper Configuration Management. (See PP. 11 and 18 of the Statement of Work.)

126. On July 21, 2010, Exhibit A at page 27 of the Contract was added. (See attached Exhibit 16.). In February and March 2010, Relator Atkins and other IAMD PO personnel recommended that much of the data listed in this exhibit be rejected. This information, plus additional information would be required to be reviewed for the critical design review that was supposed to take place in the summer of 2012. The delivery of the important data that Northrop was to produce under the contract was changed from 120 days to 45 or 60 days before the Critical Design Review (CDR). Relator Atkins knew from experience that a proper inspection of most of this data required more time then the original 120 days. Cutting that time in half was an indication to Relator Atkins that the IAMD front office did not want the reviewers to do their due diligence in reviewing the documents before the CDR. The time period allowed to carefully inspect Northrop's production was intentionally shortened by Northrop and members of the IAMD front office, so that Northrop's unfulfilled or insufficient work product would not be fully exposed. This includes (but is not limited to) the Prime Item Development Specifications, the Software Requirements Specifications and the Interface Requirements Specifications of the Contract.

VII.
PERTINENT REGULATIONS VIOLATED

127. As one of the top four military contractors of the world, Northrop Grumman knows "that those who seek public funds [are to] act with scrupulous regard for the requirements of the law," and "those who deal with the Government are expected to know

the law and may not rely on the conduct of Government agents contrary to law." (United States, ex rel. Hagood v. Sonoma Water Agency, 929 F.2d 1416 (9th Cir. 1991). "Men must turn square corners when they deal with the government" is a well known axiom of federal contracting law.

128. Northrop Grumman has not only fundamentally been violating the IAMD IBCS contract, but has violated the Federal Information Security Management Act (FISMA) of 2002, and the following which govern administration of the contract:

a. Army Regulation 25-2;
b. DODI 8510.01, DOD Information Assurance Certification and Accreditation Process (DIACAP);
c. DODD 8500.1 on Information Assurance; and
d. DODI 8500.2 on Information Assurance Implementation.

129. Pursuant to 48 C.F.R. 43.102(a), only a contracting officer acting within the scope of her authority can waive or modify a term of a government contract. The regulation mandates:

(a) Only contracting officers acting within the scope of their authority are empowered to execute contract modifications on behalf of the Government. Other Government personnel shall not-

(1) Execute contract modifications;
(2) Act in such a manner as to cause the contractor to believe that they have authority to bind the Government; or
(3) Direct or encourage the contractor to perform work that should be the subject of a contract modification.

130. Under Federal Acquisition Regulation 33.210(b), even the official contracting officer has no authority to settle, compromise, pay, or adjust any claim involving fraud. In addition, under Section 604(a) of the federal Contract Disputes Act, the Army or any other government agency has no authority "to settle, compromise, pay, or otherwise adjust any claim involving fraud."

131. Thus, Project Managers like Colonel Rasch can accept programmatic risk (cost and schedule) within reason, but only the Designated Approving Authority (DAA) of a system can accept security risks. The DAA is normally at a General Officer (GO) or Senior Executive Service (SES) level. For PM Rasch to claim that he can accept the risk of not doing Information Assurance or anything else that relates to security is false. He has no such authority.

132. The G-SIL authority to deny Defendant's hardware and software access to the government networks is clear. Army Regulation 25-2 dated 24 October 2007 (Rapid Action Revision (RAR), Issue Date: 23 March 2009, mandates at 1-4g (pg. 1): "Failure to implement proactive or corrective IA security measures, guidance, policy, or procedures may prevent system or enclave accreditation, installation, or operation and may increase system vulnerability to foreign and domestic computer network operation (CNO) activities designed to deny service, compromise information, or permit unauthorized access to sensitive information. IA or network personnel may block access to ISs that reflect poor IA security practices or fail to implement corrective measures."

133. Army Regulation 25-2 also provides at 1-5g(10) (pg. 2): "Mandates that DOD and Army-level designated approving authorities (DAAs) meet the system accreditation requirements of this regulation before fielding or testing any system that requires connection to an Army network." Thus, connections to the government network without meeting accreditation requirements are illegal, and NG was denied the attempt.

134. Army Regulation 25-2 also requires the implementation of a Configuration Management (CM) process. (See 1-5g (11) (p.2).

135. Army Regulation 25-2 also mandates at 4-8 a. (pg. 30): "All information systems will be designed to meet the IA controls as identified in DODI 8500.2 and be configured in compliance with the applicable DISA STIG or baselined system with identified changes documented as part of the accreditation process." Defendant Northrop Grumman improperly attempted to claim that STIGs were guides, and not mandatory, as part of its cover up.

136. Army Regulation 25-2 further mandates at 4-24 a. (pg. 44): "The Information Assurance Vulnerability Management (IAVM) Program is the absolute minimum standard for all ISs, not the preferred end state which is a proactive methodology of maintaining, patching, and updating systems before notification or exploitation. IAVM requires the completion of four distinct phases to ensure compliance."

137. Department of Defense Directive DoDD 8500.1 Information Assurance (IA), certified current as of April 23, 2007, directs:

> i. 4.14. All interconnections of DoD information systems shall be managed to continuously minimize community risk by ensuring that the assurance of one system is not undermined by vulnerabilities of interconnected systems.
> ii. E2.1.5. Community Risk. Probability that a particular vulnerability will be exploited within an interacting population and adversely impact some members of that population.

138. Department of Defense Instruction DODI 8500.2 Information Assurance (IA) Implementation, dated February 6, 2003, dictates:

> i. E3.2.5.7. Implementation of security-related software patches directed through the DoD IAVA program shall not be delayed pending evaluation of changes that may result from the patches.
> ii. E3.2.6. Security Configuration Specification. DISA and NSA support the Defense IA program through the development and dissemination of security implementation specifications for the configuration of IA- and IA-enabled IT products. Examples of such specifications include Security Technical Implementation Guidelines (STIG) and Security Recommendation Guides (SRG).

139. The U.S. Department of Defense Instruction DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), dated November 28, 2007, dictates:

i. 5.16.3. Plan and budget for IA controls implementation, validation, and sustainment throughout the system life cycle, including timely and effective configuration and vulnerability management.

ii. 6.3.3.2.6.1.2. A system with a CAT I weakness may not be granted an ATO (Authority to Operate).

iii. 6.3.3.2.6.1.3. A system with a CAT II weakness can be granted an ATO only when there is clear evidence that the CAT II weakness can be corrected or satisfactorily mitigated within 180 days of the accreditation decision.

iv. 6.3.4. Maintain Authorization to Operate and Conduct Reviews. Continued ATO is contingent on the sustainment of an acceptable IA posture. The DoD IS IAM has primary responsibility for maintaining situational awareness and initiating actions to improve or restore IA posture.

v. 6.3.4.1: The IAM continuously monitors the system or information environment for security-relevant events and configuration changes that negatively impact IA posture and periodically assesses the quality of IA controls implementation against performance indicators such as security incidents, feedback from external inspection agencies (e.g., IG DoD, Government Accountability Office (GAO)), exercises, and operational evaluations. [Underlined emphasis added.]

140. The system has to meet the security and configuration requirements regardless of whether IAMD has its own accreditation or if it is under the G-SIL ATO umbrella.

VIII.
DEFFENDANT'S DEVELOPMENT OF THE ENTERPRISE BATTLE COMMAND SYSTEM (EBCS)

141. While she still worked at IAMD, relator Atkins became aware that defendant Northrop Grumman was building a system similar to the IAMD Battle Command System (IBCS) that the defendant called the Enterprise Battle Command System (EBCS). Relator Atkins reviewed slides concerning the EBCS with Kelli W. Smith, the IAMD International Specialist. Both relator Atkins and Mrs. Smith concluded

that the EBCS program appeared identical to the IBCS, and that defendant Northrop Grumman would more than likely try to get its EBCS system approved for Direct Commercial Sales (DCS). This would allow defendant Northrop Grumman to sell the EBCS for millions of dollars to foreign country militaries, without the United States benefiting from the Foreign Military Sales (FMS).

142. In a meeting on May 22, 2014 Brig. Gen. Neil Thurgood the current Program Executive Officer of the Program Executive Office Missiles and Space, accused managers of defendant Northrop Grumman of focusing on building its EBCS program at the neglect of the IBCS program, including Northrop Grumman's transferring employees off of the IBCS work and onto the EBCS development. General Thurgood told the Northrup managers that he was aware of 6 such transferred individuals. Gen. Thurgood also challenged the Northrup managers present to distinguish between the software code that the government had been paying for under the IBCS contract from that of the EBCS code. None of the Northrup management present could give him an answer. Northrup managers present included Robert Jassey. Gen. Thurgood also stated that just the year before he had warned Northrop Grumman against doing this. Gen. Thurgood was obviously angry. Also present in the meeting were the IBCS Project Manager Rasch and Deputy Project Manager Achord. After the obviously angry Gen. Thurgood departed from this meeting, one of the Northrop Grumman managers or Rasch or Achord stated that, "Our smoke and mirrors have worked before," and that they just had to think of a way to proceed.

143. Thus, both relators verily believe that defendant Northrop Grumman has knowingly and intentionally refused to build the necessary security requirements into the

IBCS according to the contract and regulations, while accepting millions of dollars of federal money for that purpose, while building its privately owned, nearly identical system for the purpose of selling it for profits of millions of dollars.

IX.
BILLING AND CERTIFICATION DOCUMENTS

144. At this point in the summer of 2014, Relators do not have access to the specific documents regarding the payment requests and false certifications as such documents are in the exclusive possession and control of the Defendant, and the Department of Defense.

X.
THE FALSE CLAIMS ACT

145. The federal FCA makes it unlawful for any person to directly or indirectly deceive the government and cause it to pay money. *See* 31 U.S.C. §3729 et seq. Relators allege liability under three of the FCA's seven liability provisions.

146. First, Relators allege liability under 31 U.S.C. §3729(a)(1)(A), which imposes liability when any person "knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval."

147. Second, Relators allege liability under 31 U.S.C. §3729(a)(1)(B), which imposes liability when a person "knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim."

148. Third, Relators alleged liability under 31 U.S.C. §3729(a)(1)(C), which imposes liability when a person "conspires to commit a violation of subparagraphs (A) or (B)" or other provisions of the FCA.

149. As defined under 31 U.S.C. §3729(b), "knowing" and "knowingly" means that a person: (1) has actual knowledge of the information; (2) acts in deliberate ignorance of the truth or falsity of the information; or (3) acts in reckless disregard of the truth or falsity of the information.

150. Under 31 U.S.C. §3729(c), a claim includes "any request or demand, whether under a contract or otherwise, for money or property which is made to a contractor, grantee, or other recipient if the United States Government provides any portion of the money or property which is requested or demanded, or if the Government will reimburse such contractor, grantee, or other recipient for any portion of the money or property which is requested or demanded." Under this language, claims submitted to Federal agencies like the Army are claims presented to the federal government and therefore give rise to liability under the FCA.

151. Under the FCA, "the term 'material' means having a natural tendency to influence, or be capable of influencing, the payment or receipt of money or property." 31 U.S.C. §3729(a)(4).

152. The FCA mandates penalties of not less than $5,500 and not more than $11,000 per occurrence, plus mandatory treble damages. 31 U.S.C. §3729(a).

153. The FCA enforces certain principles that apply when one deals with the government. These include the fact that *caveat emptor* is replaced by a duty to "turn square corners" and be honest and forthright with the government, and to deliver goods and services precisely according to the specifications mandated.[3]

---

[3] *Caveat emptor* does not apply when dealing with the government. As stated long ago by Justice Holmes, "[m]en must turn square corners when they deal with the government." *Rock Island, Arkansas & Louisiana R.R. v. United States,* 254 U.S. 141, 143, 41 S.Ct. 55, 65 L.Ed. 188 (1920); *see also Fed. Crop Ins. Corp. v. Merrill,* 332 U.S. 380, 385 (1947) (setting out the fact that "'Men must turn square corners when they deal

COUNT I.
31 U.S.C. §3729(a)(1)(A)

154. Plaintiffs re-allege the above paragraphs. Defendant had knowledge that its Anti-Tamper, Information Assurance, and Configuration Management components failed to meet the requirements of the IAMD contract, as well as Army and Department of Defense Regulations and other federal laws, and nonetheless presented claims for payment to the Army, which claims were thereby false or fraudulent because they were factually false, and/or falsely certified (expressly and/or impliedly) compliance with all contract requirements material to the government's obligation to pay. Defendant also knowingly attempted to evade and cover up its failures to provide those valid security measures as required.

155. Despite this knowledge, Defendant submitted many claims for payment, and were paid millions of dollars thereon, in violation of the False Claims Act, 31 U.S.C. §3729(a)(1)(A), by knowingly presenting false or fraudulent claims for payment by the United States. Based upon information, Relators believe that Defendant was paid in excess of $630 million through 2012 on the IAMD IBCS contract.

COUNT II.

---

with the Government,' does not reflect a callous outlook. It merely expresses the duty of all courts to observe the conditions defined by Congress for charging the public treasury"). This principle is codified in the government acquisition term of art known as "cost and pricing data," 10 U.S.C. § 2306a(h)(1) and 41 U.S.C. § 3501, which requires affirmative disclosure of all relevant information. Important here, the principle is also widely applied in FCA actions. *See, e.g., U.S. v. Rogan,* 517 F.3d 449, 452 (7th Cir. 2008); *U.S. ex rel. Compton v. Midwest Specialties, Inc.,* 142 F. 3d 296, 302-305 & n.4 (6th Cir. 1998) (setting out that "parties that contract with the government are held to the letter of the contract – irrespective of whether the contract terms appear onerous from an *ex post* perspective, or whether the contract's purpose could be effectuated in some other way" and thus "the 'square-corners' rule applies fully in the False Claims Act context"), *following United States v. Aerodex, Inc.,* 469 F.2d 1003, 1007 (5th Cir. 1972) (noting that "[t]he mere fact that the item supplied under contract is as good as the one contracted for does not relieve defendants of liability")(emphasis added); *U.S. v. Rivera,* 55 F.3d 703, 709 (1st Cir. 1995) (setting out that "[b]y attaching liability to the claim or demand for payment [under (a)(1)], the [FCA] encourages contractor [sic] to 'turn square corners when they deal with the government'"), *quoted and followed by Machado v. Sanjurjo,* 559 F.Supp.2d 167, 174 (D. Puerto Rico 2008); *United States v. Bourseau,* No. 03-cv-907, 2006WL2961105, *1 & n.1 (S.D. Cal. 2006).

31 U.S.C. §3729(a)(1)(B)

156. Plaintiffs re-allege the above paragraphs. Defendant also violated the False Claims Act at 31 U.S.C. §3729(a)(1)(B) by knowingly making, using, or causing to be made or used, false records or statements that were material to a false or fraudulent claim, including without limitation when they expressly represented and/or certified that the work that they were billing for under the contract was in compliance with the contract terms, and/or in compliance with Department of Defense regulations, rules or instructions, and all federal laws. These certifications were made on Request for Progress Payment SF1443 forms and/or other forms, as well as the IAMD contract that Defendant signed. In addition, based upon Relators' information and belief, representatives of the Defendant made false records or statements material to false or fraudulent claims in presentations to the Army's Honorable Heidi Shyu, and other government representatives, in meetings where Defendant's representatives alleged progress and compliance made under the Contract. The requests for payment, the contract, the certifications of compliance and the described representations were all material to the Government making multiple payments to Defendant under the contract for years.

COUNT III.
31 U.S.C. §3729(a)(1)(C)

157. Plaintiffs re-allege the above paragraphs. Defendant also violated the False Claims Act at 31 U.S.C. §3729(a)(1)(C), when its representatives conspired with members of the Army who did not have authority to change or modify the Contract to fraudulently cover up and attempt to evade Anti-Tamper, Information Assurance and Configuration Management requirements under the contract and federal law, in order to have Defendant's payments under the contract continue.

COUNT IV.
31 U.S.C. §3729(a)(1)(G)

158. Plaintiffs re-allege the above paragraphs. Defendant also violated the False Claims Act 31 U.S.C. §3729(a)(1)(G), by knowingly making, using or causing to be made or used, a false record or statement material to an obligation to pay money to the United States and/or knowingly concealing or knowingly and improperly avoiding an obligation to pay money to the United States, because it, through its representatives or employees, knew that it was accepting substantial sums of payments under the contract when it was not abiding by the contract terms and federal regulations in respect to Information Assurance and Anti-Tamper protections, and Configuration Management.

THEREFORE, Plaintiffs request judgment against the Defendant pursuant to the the False Claims Act for:

a. An amount three times the amounts wrongfully claimed and taken by Defendant.
b. Penalties up to $11,000 per false claim;
c. Injunction relief for the United States to stop the fraud and fraudulent conduct of Defendant;
d. All expenses incurred by the United States in pursuing this action;
e. A recovery for Relators, including their attorney fees and costs, as provided by the False Claims Act; and
f. All interest and costs allowed by law.

PLAINTIFFS REQUEST TRIAL BY JURY.

DATED: 18 AUGUST 2014

Respectfully Submitted,

Frederick M. Morgan, Jr. (0027687)
Trial Attorney
Jennifer M. Verkamp (0067198)
Morgan Verkamp LLC
35 East Seventh Street, Suite 600
Cincinnati, OH 45202
(513)651-4400
rick.morgan@morganverkamp.com
jverkamp@morganverkamp.com

D. Anthony Mastando
License No.: ASB-0893-X32B)
Eric J. Artrip
License No. ASB-9673-168E
Attorneys for Relators
Mastando & Artrip, LLC
302 Washington St., Suite 302
Huntsville, Alabama 35801
(256) 532-2222
tony@mastandoartip.com
eric@mastandoartip.com

Gerald C. Robinson
Attorney for Relators
Gerald Robinson Law Firm, PLLC
5600 W. 70th Street, Suite 200
Minneapolis, MN 55439
(612) 803-5981
MN LIC 212787
gerald.robinson@gcrobinsonlaw.com

Brian Wojtalewicz
Attorney for Relators
Wojtalewicz Law Firm, Ltd.
139 N Miles St., PO Box 123
Appleton, MN 56208-0123
(320)289-2363
MN LIC 118369
brian@wojtalewiczlawfirm.com